

### **Remark**

Applicants respectfully request reconsideration of this application as amended. Claims 1-8, 10 and 13-17 have been amended. No Claims have been canceled. Claims 18-20 have been added as New. Therefore, claims 1-20 are now presented for examination.

### **Claim Objections**

The claims are objected to for the following minor informality:  
Claim 7 repeats “the”. The claim is amended.

### **35 U.S.C. §112 Rejection**

The Examiner has rejected claim 8 under 35 U.S.C. §112, second paragraph, as indefinite with respect to the naming of certificates. The claim is amended.

### **35 U.S.C. §102 Rejection**

#### *Hur*

The Examiner has rejected claims 1-4, 6-11 and 13-16 under 35 U.S.C. §102 (e) as being anticipated by Hur, U.S. Patent No. 7,181,620 (“Hur”). Hur shows an authentication system using a cryptographic key approach. In Hur, there are several keys with overlapping names that cover a variety of different possible scenarios. The keys include a realm key, a shorter-lived key, a longer-lived key, a session key, a device symmetric key etc. It would appear that all keys are either provided by a key management server or are built into a network device at the manufacturer. Once the

appropriate keys are distributed by the key management server, then they can be used for various activities and, in particular, for peer-to-peer communications.

Claim 1 has been amended to clarify the operations that are involved and to recite actors as appropriate. Applicants do not believe that the claim has been narrowed.

First, Applicants respectfully point out that Claim 1 mentions three actors: a user terminal; an access point of an access network, and an Internet Service Provider. While the Examiner has pointed to various general illustrations of network configurations in Hur, there is simply no ISP and it is not clear that there is an access point. Instead, Hur's network appears to be populated with peer nodes and a few servers, such as the key management server. Accordingly, these features of the claim are not anticipated.

Second, Applicants respectfully point out that Claim 1 refers to a service certificate. The service certificate includes a subscription identifier. This element points out another distinction from Hur. Hur is not concerned with subscriptions, but with security. As there is no ISP with which to subscribe, there is similarly no subscription.

Third, Applicants respectfully point out that Claim 1 refers to a CRL maintained by the ISP. In Hur, it would appear that any CRLs (none are expressly mentioned) would be maintained by the key management server, but the key management server is not an ISP and does not provide subscriptions.

For all of these reasons, Claim 1 is not anticipated. As is clear from the explanation above, the ISP is not just a difference in terminology, but a difference in substantive nature of the type described by all of the other limitations in the claim. The same reasoning applies also to Claim 13.

Claim 6 presents a different aspect of the invention. In Claim 6, an access point either determines the validity of a certificate or sends the certificate to an ISP to

determine the validity. This is done based on a determination made at the access point. The Examiner has found nothing similar in Hur. The Examiner has only found a description of the operations of the key management server that control and check all certificates. As to sending the certificate to an ISP, the Examiner cites to Columns 10 and 14 which both describe a process run entirely with the key management server. There is no suggestion of a second entity and certainly no suggestion of an ISP.

Claim 10 presents a user terminal that stores two certificates. These certificates differ fundamentally from those of Hur. The first certificate is used to authenticate the user terminal with the ISP and the second certificate is used to authenticate the user terminal to an access point. Hur has no such distinction. As mentioned above, in Hur all of the keys come from the key management server and are authenticated and maintained there. There are no ISPs and no access points. Accordingly, Claim 10 is also not anticipated.

The remaining claims not discussed above are all dependent on one of the claims discussed above and are believed to be allowable therefore, *inter alia*.

### **35 U.S.C. §103 Rejection**

#### *Hur and RFC*

The Examiner has rejected claims 5, 12 and 17 under 35 U.S.C. §103 (a) as being unpatentable by (“Hur”) and “RFC 1661: The Point-to-Point Protocol (PPP)”. This rejection relies on the Hur rejection and is traversed for the reasons provided above, *inter alia*.

### **Conclusion**

Applicants respectfully submit that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicants respectfully request the rejections be withdrawn and the claims as amended be allowed.

### **Invitation for a Telephone Interview**

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

### **Request for an Extension of Time**

Applicants respectfully petition for a Three-Month extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a). Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17(a) for such an extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: April 10, 2008



---

Gordon R. Lindeen III  
Reg. No. 33,192

1279 Oakmead Parkway  
Sunnyvale, California 94085  
(303) 740-1980